

EXHIBIT 5666

Thanks.

On Sep 23, 2015 6:42 PM, "Adrian Ludwig" <[REDACTED]@google.com> wrote:

#2 is the issue that was raised by Samsung

On Wed, Sep 23, 2015, 6:28 PM Ashish Pimplapure <[REDACTED]@google.com> wrote:

We do have an agenda item on upgrades in general, including security updates. Will include Adrian for that portion.
@Adrian: re: "tighter controls around installation of apps from outside of Google Play," did you mean:

- 1) installs during setup / oobe that are offered to the user, or
- 2) subsequent installs that are initiated by the user?

For #1, we have ongoing conversations with Samsung to use Play Auto Installs.

On Wed, Sep 23, 2015 at 6:02 PM, Hiroshi Lockheimer <[REDACTED]@google.com> wrote:

+Ashish

They're here on Friday. Ashish do you know if this will be a topic? If not maybe we should make it one and have Adrian attend that portion. I also think it's good to brainstorm openly with them incl binary updates etc.

On Wed, Sep 23, 2015 at 4:21 PM, Adrian Ludwig <[REDACTED]@google.com> wrote:

Just us -- DJ mentioned an upcoming visit by Injong and Peter. Is that good time to try to have some proposals for closer collaboration? (I'm not aware of when that is happening and/or what might be on the Agenda.)

Currently, the three areas where closer collaboration would be fruitful are (1) updates (2) vulnerability information sharing and coordination and (3) PR / marketing coordination.

I would also like to be able to have a meaningful conversation about binary updates and/or tighter controls around installation of apps from outside of Google Play, but those both seem like areas where we currently lack internal alignment / commitment.

Other thoughts?

Adrian

On Wed, Sep 23, 2015, 7:53 AM Hiroshi Lockheimer <[REDACTED]@google.com> wrote:

Hi DJ, I'm glad to hear your team is keen to discuss security with us. This is something we've been thinking about for many years and we welcome the collaboration. I've looped in Adrian -- who Henry knows -- who is our main point of contact on issues related to security. Thanks.

On Wed, Sep 23, 2015 at 2:19 AM, 고동진 DJ Koh <[REDACTED]@samsung.com> wrote:

Hi Hiroshi,

I am sure you are aware of the recent Xcode security breach that has made about three dozens of Chinese apps, including

WeChat and Didi Kuaidi, on Apple Store embed malware in these apps (<http://www.wsi.com/articles/apple-targeted-as-hackers-infect-popular-chinese-mobile-apps-with-malware-1442750168>). When this breach happened, Apple just deleted these compromised apps from their store and this blocked the propagation of the compromised apps. This is a simple and effective action, however, such an action does not work very well on Android due to Android's app distribution mechanism allowing side loading and self-signed apps.

Since Android has been an open platform and has allowed side loading for maximum freedom for developers, I believe it has provided good value to attract developers and grow the community faster. However, we also suffer from the consequence of them. I think it is time to serious think about the security baseline of Android and how to improve it. Our competitor has better and easier security controls such as developer signing certificate, App Store only app distribution with no side loading and no support for jailbroken devices, whereas rooting is generally accepted in the Android community in the spirit of open platform.

As we are collaborating on the monthly security updates to better respond to security breaches and address software vulnerabilities faster, we also need to think of building a better security framework to improve overall security of Android OS and to provide easier controls to mitigate security vulnerabilities.

It would be greatly appreciated if Google takes the lead to build up a security improvement plan for Android and share it with us. We may also work together to define a series of actionable items to achieve this goal, which may affect the current Android architecture. Please have a fruitful discussion during Injong and Peter's visit.

Warmest regards,

DJ

The above message is intended solely for the named addressee and may contain trade secret, industrial technology or privileged and confidential information otherwise protected under applicable law including the Unfair Competition Prevention and Trade Secret Protection Act. Any unauthorized dissemination, distribution, copying or use of the information contained in this communication is strictly prohibited. If you have received this communication in error, please notify the sender by email and delete this communication immediately.

상기 메일은 지정된 수신인만을 위한 것이며 부정경쟁 방지 및 영업비밀 보호에 관한 법률을 포함하여 관련 법령에 따라 보호의 대상이 되는 영업비밀, 산업기술 등을 포함하고 있을 수 있습니다. 본 문서에 포함된 정보의 전부 또는 일부를 무단으로 제3자에게 공개, 배포, 복사 또는 사용하는 것은 엄격히 금지됩니다. 본 메일이 잘못 전송된 경우, 발신인에게 알려 주시고 즉시 삭제하여 주시기 바랍니다.

--

Adrian Ludwig
Android Security
[REDACTED]@google.com

--

Adrian Ludwig

CONFIDENTIAL

GOOG-PLAY-000421172

EXHIBIT 5666-002

